PATENT ABSTRACTS OF JAPAN

(11)Publication number : 64-028672
(43)Date of publication of application : 31.01.1989

(51)Int.Cl. G09C 1/00
G06F 15/21
// H04L 9/00

(21)Application number : 62-183278
(22)Date of filing : 24.07.1987

(71)Applicant : HITACHI LTD
(72)Inventor : NAGAI YASUHIKO
TAKARAGI KAZUO
SASAKI RYOICHI

(54) AUTHENTICATION SYSTEM FOR ELECTRONIC TRANSACTION

(57)Abstract:
PURPOSE: To realize the high-speed efficient processing on operation by using a public key for deciphering whose length is shorter than that of an encipherment secret key in an electronic transaction authentication system using a public key encipherment system.
CONSTITUTION: In the processing system where documents are substituted for electric information to perform electronic transactions, data indicating contents of a transaction text is enciphered by the public key encipherment system to generate authentication data. Enciphered authentication data is deciphered by the public key for deciphering to confirm the authentication data. At this time, a public key whose length is longer than that of the encipherment secret key is adopted as the public key for deciphering. A high-speed remainder calculation system using a remainder table is adopted to generate the authentication data. A conventional system where a quotient is obtained and is subtracted from a dividend is adopted to generate the authentication data. Consequently, the speed of the confirmation processing of authentication data is increased because the length of the public key for deciphering is longer than that of the encipherment secret key.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭64－28672

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和64年(1989)1月31日
G 09 C 1/00		7368－5B	
G 06 F 15/21	310	Z－7230－5B	
// H 04 L 9/00		Z－7240－5K	審査請求　未請求　発明の数 2　(全4頁)

㊹発明の名称　電子取引用認証方式

㉑特　願　昭62－183278

㉒出　願　昭62(1987)7月24日

㉒発明者　永井　康彦　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉒発明者　宝木　和夫　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉒発明者　佐々木　良一　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地

㉔代理人　弁理士　小川　勝男　外1名

明　細　書

1．発明の名称

電子取引用認証方式

2．特許請求の範囲

1．書類を電気的情報に置き換えて、電子的に所望の取引を行ない、かつ取引文の内容を示すデータを公開鍵暗号方式を用いて暗号化することで認証データを作成，復号することで認証データの確認をする電子取引用認証方式において、復号用公開鍵には、暗号化用秘密鍵よりも短い鍵長のものを採用し、認証データ作成には、剰余テーブルを用いた高速剰余計算方式、認証データ確認には従来方式の商を求めて被除数から減算する方式を採用することにより、認証データ作成・確認処理の高速化を可能とすることを特徴とする電子取引用認証方式。

2．ホスト対端末が1：n（n：正整数）であるような通信ネットワークを持つ電子取引方式において、ホスト側や取引頻度の高い端末側では認証データ作成用に上記剰余テーブルを用いた剰余計算方式を採用することを特徴とする電子取引用認証方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、書類をコンピュータのメッセージに置き換え、電子的に商取引を行ない、公開鍵暗号方式による取引データの認証を行なう電子取引用認証方式において、特にホスト1に対し相手端末がnであるような通信ネットワーク上の認証処理の高速化，高効率化に適する。

〔従来の技術〕

従来、商取引による契約交渉は、サイン・印鑑によりその正当性を認証している。この作業をデジタル通信を利用した電子取引で実現する方法が考案されているが、サイン・印鑑のデータをそのままデジタル信号に変換して使用することは、取引の信頼性の面から問題を生じる。これは、サイン・印鑑のデジタル信号化されたデータは、簡単にその複製を作成することができるため、その複製物により不正な取引を行なうことが容易なため

である。そこで、サイン・印鑑のデータの単純なデジタル信号化に変わる手段としてデジタル署名を用いる手段が有力とされている。デジタル署名とは、認証を行ないたい情報（取引当事者の氏名や取引内容）に暗号化処理を行なって作成した暗号文で、この暗号化の際に用いた暗号化鍵を知らない第三者には、作成することが困難なものであるという事実から、その作成者を認証・特定化するものである。

現在、このデジタル署名を実現するために最も有力な暗号方式は、公開鍵暗号方式である。公開鍵暗号方式では、データ（平文）を暗号化する鍵と暗号化されたデータ（暗号文）を復号する鍵の値が異なっているという特徴がある。そのため、暗号化鍵は秘匿し、復号鍵を公開しておくことにより、任意の第三者に暗号化鍵を秘匿したままで認証をさせることができる（（財）日本情報処理開発協会：「コンピュータ・システムのセキュリティ技術の開発に関する調査研究報告書」昭和５９．３参照）。

〔発明が解決しようとする問題点〕

従来、上記公知例に代表されるような公開鍵暗号方式を用いたデジタル署名には、一般に公開鍵暗号方式が多倍長の剰余計算を計算単位とし、計算量が多いため処理速度の点で実用化が困難であるという問題があり、運用面での効率的な実用化方法も検討されていない。

本発明の目的は、多倍長剰余算を計算単位とする公開鍵暗号方式を用いた電子認証方式において、運用面での高速，高効率処理を実現し、実用的な電子取引用認証方式を提供することにある。

〔問題を解決するための手段〕

上記目的を達成するため、本発明による電子取引用認証方式では、公開鍵暗号方式の公開鍵に秘密鍵より鍵長の短いものを採用する。公開鍵は、関係者に公開される暗号鍵であるため、鍵長を短くしても実用上安全性に問題はない。これにより、認証データ確認のための計算量を減少させる。また、電子取引を行なう通信ネットワーク内で、取引文データが集中するホストや、取引頻度の高い端末において認証データ作成に剰余テーブルを用いた多倍長剰余計算高速化方式を採用する。

〔作　用〕

公開鍵に秘密鍵よりも短い鍵長のものを採用することにより、認証データ確認処理の計算量を減少させ、高速化が達成できる。また、取引データの処理量が多いホストや端末において認証データ作成処理に剰余テーブルを用いた剰余計算高速化方式を採用することで、通信ネットワークトータルとしての取引の高速化，高効率化が達成できる。

〔発明の実施例〕

以下、本発明の一実施例について、その構成，動作を第１図及び第２図を用いて説明する。

第１図は、投資家（端末）と証券会社（ホスト）を通信ネットワークで結ぶ株式売買システムに本発明を適用した場合の構成を示している。

公開鍵暗号処理用暗号機としては、比較的低速ではあるが小型で実現できる方式，高速ではあるがメモリ容量を多く必要とする方式という２つの方式のものがある。投資家側端末では、取引頻度が少ないことから、従来の比較的低速の公開鍵暗号処理用暗号機Ａを用い、認証データの作成・確認を行なう。一方、証券会社であるホスト側では、認証データの確認用の公開鍵は作成用秘密鍵よりも鍵長が短いことから計算量が少ないため、認証データの確認には低速の暗号機Ａを採用し、認証データ作成には、剰余テーブルを用いた高速処理用暗号機Ｂを用いる。

第２図は、端末側，ホスト側の構成要素及び処理フローを示している。

ステップ１：まず投資家側端末１０１において、注文伝票の内容を示すデータ及び取引状況を示すデータ等より認証データ原文作成器１０２より認証原文を作成し、また、記憶装置１０３より投資家側秘密鍵を暗号機Ａ１０４にロードして投資家側認証データを暗号化することにより作成する。

ステップ２：次に作成された認証データを記憶装

置１０３に登録すると共に通信制御装置１０５より証券会社側へ送信する。

ステップ３：証券会社側は、通信制御装置１０６より投資家の認証データを受信し、記憶装置１０７へ登録する。

ステップ４：次に暗号機Ａ１０８に記憶装置より認証データ及びそのデータの送信元である投資家に対応した公開鍵をロードし、認証データを復号して原文を得る。

ステップ５：得られた認証データ原文を比較器１０９により確認し、妥当であれば証券会社側の認証データ原文を作成器１１０より作成する。

ステップ６：ホスト側秘密鍵を記憶装置１０７より暗号機Ｂ１１１にロードし、会社側認証データを作成する。

ステップ７：通信制御装置１０６より投資家側へ認証データを送信する。

ステップ８：会社側認証データを通信制御装置１０５より受信し、記憶装置１０３よりホスト公開鍵を暗号機Ａ１０４にロードして認証データの復号を行なう。

ステップ９：復号結果である認証原文を比較器１１２より認証し、妥当であれば認証データを記憶装置１０３に登録する。

以上により作成・確認した双方の認証データを双方が保管しておくことにより、本取引は保証される。なお、本実施例では２種類の暗号機Ａ，Ｂを使用したが、剰余テーブルを用いた高速化方式が、今後小型、低コストで実現可能になれば、全てを暗号機Ｂにすることにより一層高速化が望める。また、本方式は、電子取引における認証機能だけでなく、一般的に公開鍵暗号方式を応用した各種機能を実現する場合においても有効である。

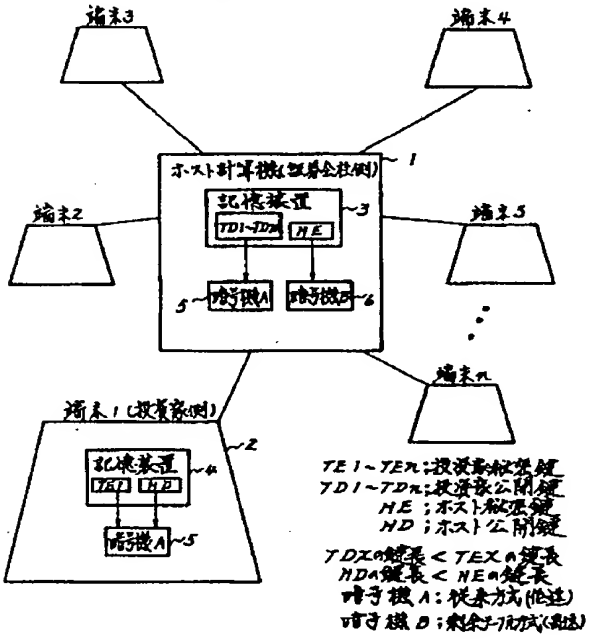
〔発明の効果〕

本発明によれば、復号用公開鍵には暗号化用秘密鍵よりも短い鍵長のものを採用したことにより、認証データ確認処理の計算量を減少させ、高速化が実現でき、また、多量の取引文を処理するホスト側や取引頻度の高い端末側において認証データ作成のため剰余テーブルを用いた公開鍵暗号高速処理方式を採用することにより、通信ネットワークトータルとしての取引の高速化，高効率化を実現できるという効果がある。

４．図面の簡単な説明

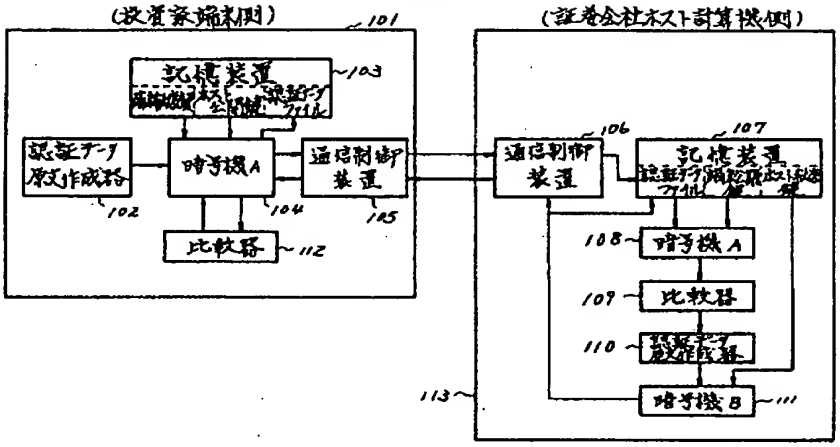
第１図は、本発明による株式売買システムの一構成図、第２図は、その構成要素及び処理フロー図である。

第１図



代理人　弁理士　小川勝男

第２図


（投資家端末側）
101
記憶装置
103
認証データ原文作成部
暗号機A
通信制御装置
102
104
105
比較器
112
（証券会社ホスト計算機側）
通信制御装置
106
記憶装置
107
108
暗号機A
109
比較器
110
113
暗号機B
111